IN THE CLAIMS:

A status of all the claims of the present Application is presented below:

1.   **(Currently Amended)**   A network having [[a]] an intrusion protection system, comprising:

a network medium;

a management node connected to the network medium and running an intrusion prevention system management application; and

a plurality of nodes connected to the network medium and running an instance of an intrusion protection system application, at least one of the nodes having an identification assigned thereto based on a logical assignment grouping one or more of the plurality of nodes, each node sharing an identification being commonly vulnerable to at least one network exploit.

2.   **(Original)**   The network according to claim 1, wherein the management node is operable to originate a security update that is transmitted to each node sharing the identification, any remaining nodes not sharing the identification being excluded from receiving the update.

3.   **(Original)**   The network according to claim 1, wherein a plurality of identifications are respectively assigned to one or more of the plurality of nodes.

4.   **(Original)**   The network according to claim 1, wherein the identification is an Internet Protocol multicast group identification.

5.   **(Currently amended)**   The network according to claim 2, further comprising:

a plurality of network mediums; and

at least one router, each of the management node and the plurality of nodes each respectively connected to one of the plurality of network mediums in the network, the router

disposed intermediate the plurality of network mediums and operable to forward the security update from the network medium having the management node connected thereto to any nodes connected to the remaining network mediums and sharing the identification.

6.   **(Original)**   The network according to claim 5, wherein the router determines whether any of the plurality of nodes connected to the remaining network mediums share the identification through implementation of the Internet group management protocol.

7.   **(Original)**   The network according to claim 1, wherein the network medium is an Ethernet.

8.   **(Original)**   The network according to claim 1, further comprising a network-based intrusion protection system appliance dedicated to filtering inbound and outbound data frames transmitted across the network medium.

9.   **(Original)**   The network according to claim 8, wherein the network-based intrusion protection system appliance interfaces with the network medium via a network interface card operating in promiscuous mode.

10.   **(Original)**   The network according to claim 8, wherein the network-based intrusion protection system appliance shares the identification.

11.   **(Withdrawn)** A method of transmitting an update message to a subset of nodes of a plurality of network nodes, comprising:

generating the update message by a management node of the network;

addressing the update message to a network address shared by the subset of nodes of the network;

transmitting the update message; and

receiving and processing the update message by the subset of nodes.

12.   **(Withdrawn)** The method according to claim 11, wherein addressing the update message to a network address shared by the subset of nodes further comprises addressing the update message to an Internet protocol multicast group identification, the subset of nodes belonging to a host group assigned to the multicast group identification.

13.   **(Withdrawn)** The method according to claim 11, wherein transmitting the update message throughout the network further comprises:

transmitting the update message on a network medium on which the management node is connected;

receiving the update message by a router terminating the network medium on which the management node is connected; and

forwarding, by the router, the update message to any nodes included in the subset of nodes on a second network medium terminated by the router.

14.   **(Withdrawn)** The method according to claim 11, wherein transmitting the update message to a subset of nodes further comprises transmitting the update message to one of at least an intrusion protection system node and a network-based intrusion protection system appliance.

15.   **(Withdrawn)** The method according to claim 11, wherein generating the update message further comprises generating a command and security update message.

16.   **(Withdrawn)** A computer-readable medium having stored thereon a set of instructions to be executed, the set of instructions, when executed by a processor, cause the processor to perform a computer method of:

generating, by the computer, a message addressed to a subset of nodes on a network;

transmitting the message on a network medium of the network to the subset of nodes;

receiving the message by a router terminating the network medium; and

forwarding, by the router, the message to any nodes included in the subset of nodes on a second network medium terminated by the router.

17.   **(Withdrawn)** The computer readable medium according to claim 16, wherein the computer method of transmitting the message on a network medium of the network to the subset of nodes further comprises transmitting the message on the network medium of the network to a subset of nodes belonging to a host group assigned to an Internet protocol multicast group identification, the update message addressed to the Internet protocol multicast group identification.